**Amendments to the Specification**

Please amend the title to read:

System and Method for Thwarting Identity Theft and Other Identity Misrepresentations

Please replace the Abstract with the following:

Registered users including businesses attach a one-time-use identity verifier to as many financial and other transactions as they choose to protect themselves from identity thieves. They may also attach a security message to any identity verifier to ensure that a thief cannot steal a registered user's check from a mailbox and use the unused identity verifier. By using one list for all of a person's transactions, applications for new credit by identity thieves are also prevented. All of this is made possible by allowing the identity verifiers to be approved nonsequentially.

Please replace the paragraph beginning at page 1, line 13, with the following:

Identity crimes are a significant problem in society. Identity crimes include identity theft, identity fraud, identity cloaking, check counterfeiting, and other crimes. Some specific examples of identity crimes include credit card theft, check theft, medicare fraud, ATM card theft, and minors using fake identifications to obtain admittance to a bar or adult-only Internet sites. Many other examples of identity crimes abound around us. Despite new laws designed to combat identity crimes, it is still easy for a criminal to take out loans in someone else's name, to run up enormous credit card debts and tap into bank accounts.

Please replace the paragraph beginning at page 2, line 15, with the following:

Another example of a situation in which verifying a person's identity is important is in preventing children from entering adult-only ~~adult only orientated~~ establishments.[[,]] For example, bars and nightclubs often need to determine the age of a patron to ensure that the patron is not a minor. Typically these establishments use a patron's driver's license to ascertain their age. However, minors often obtain fraudulent drivers licenses by inserting their photograph into a stolen or otherwise obtained driver's

license of an adult. Similar methods may be used to falsely assert an older age for purchasing cigarettes or alcohol. Use of fingerprint or other recognition equipment is typically too expensive for these establishments and therefore enforcement of the laws is difficult.

Please replace the paragraph beginning at page 5, line 7, with the following:

Figure 1 illustrates one embodiment of a computer system in accordance with the present invention. The remote terminal 200 communicates through a communications network 158 with a server computer 100. An input module 206 is connected to the server computer 100 ~~102~~.

Please replace the paragraph beginning at page 11, line 3, with the following:

The identity verification ~~verifier~~ process may be used for checks (mailed, in person, over the Internet, over the telephone), credit card transactions (mailed, in person, over the Internet, over the telephone), loan applications, opening bank or credit card accounts, preventing phone slamming or cramming, carding patrons in bars, ensuring that adult-only ~~adult only~~ sites on the Internet are not visited by children, preventing Medicare fraud, authorizing automatic bill payments by check or credit card, and verification of identities without photographs.

Please replace the paragraph beginning at page 11, line 20, with the following:

Turning now to Figure 4a, the generate operation 400 involves obtaining or generating a list of identity verifiers or identification verifiers (idv's). An identification verifier is any n-digit string of random characters, symbols or numbers. For example an identification verifier could be a five-digit ~~five-digit~~ number like 83604 or 01781. Alternatively, an identification verifier could be a six-digit ~~six-digit~~ combination of characters, symbols and numbers such as B#1?C%.

Please replace the three paragraphs beginning at page 13, line 1, with the following:

In a preferred embodiment of the methodology of the invention, the idv list is massaged to eliminate the problem of any random number repeating itself too soon

in the list. In other words, a number or string of characters used for an idv may be repeated as an idv later in time. However, a "relevant range" must be defined to make sure that the same number or string of characters is not used too close in a list to each other. For example, a relevant range could be defined as 60 days. This means the method for generating idv's must ensure that in a 60-day ~~60-day~~ period, assuming an average number of transactions, no two idv's will be the same. Modifying the size of the replenishment list (later list) can enforce this constraint.

It is also within the scope of the methodology of this invention for the idv lists to be obtained from an entity other than the entity that owns or runs the identity verification system. For example, the ~~example the~~ idv lists could be generated off site from the server computer 100 and downloaded or otherwise inputted into the database 210.

Once the idv list is generated, identical copies of it are given to the registered user and attached to the registered user's record by the entity that runs the identity verification system. ~~it is given to the registered user.~~ The registered user can store the list of idv's on a password-protected ~~password protected~~ electronic calculator-like memory device which functions as a storage and access device for the list. Alternatively, the list can be stored on paper.

Please replace the three paragraphs beginning at page 14, line 5, with the following:

In a preferred embodiment the registered user decides which information will be supplied to the record. Examples of information that could be provided are age, name, middle name, phone numbers, date of birth, social security number, drivers license number, credit card numbers, and banking account numbers. In a preferred embodiment at least one existing numerical identifier is received into the record. It is noted that this information including changes in numerical identifiers should be updated from time to time as may be necessary.

A numerical identifier is any code, number or symbol typically associated with a particular person but that could be associated with more than one person. Examples[[,]] of numerical identifiers are social security number, drivers license number,

credit card numbers, banking account numbers (as long as the routing number is included), phone numbers, etc.

Some of these numerical identifiers are shared between two or more people. For example, a couple sharing a checking account results in both individuals being associated with the same numerical identifier (the checking account number). These shared numerical identifiers can be made unique to a particular person by assigning a suffix to the shared numerical identifier. For example, the husband in the above example could be assigned suffix 1 such as a number 01, and the wife could be assigned suffix 2, such as number 02. By including the suffix with the original numerical identifier, a made-unique ~~made unique~~ numerical identifier is created.

Please replace the paragraph beginning at page 15, line 1, with the following:

Assigning suffix operation 403 determines whether a uniqueness suffix is required, and, if ~~and if~~ so, assigns a suffix. This suffix may be stored in the uniqueness suffix column as shown in Figure 7.

Please replace the paragraph beginning at page 15, line 12, with the following:

Figure 6 is an example partial record stored in the database 210 and associated with a particular registered user. The right-most ~~right most~~ column of the record in Figure 6 contains personal information about the registered user. The left columns each represent a particular category of requesting party such as bank, retailer, tavern, phone company, purchaser, car dealer, etc. There is also a miscellaneous catchall ~~catch all~~ column entitled "other". For each of these left columns, a check mark is placed in the rows for which the indicated information can be released. So, for example, if the requesting party is a tavern, then the only information that can be provided to the requesting party is the age of the registered user. On the other hand, this particular registered user has indicated in Figure 6 that if the requesting party is a bank, then the name, work phone, address, city, state, zip, social security number and middle name may be provided to the requesting party.

Please replace the paragraph beginning at page 16, line 9, with the following:

Linking idv's operation 408 of Figure 4a links the list of idv's from the generating operation 400 to the registered user's ~~party's~~ record. This record is preferably stored in a database 210. Figure 8 illustrates three example rows of entries in a database 210. Each row represents a single registered user's record. The first column is entitled "relative record number" and the numbers in this column are numbers that identify the record. The second column is entitled "list of transactions that require an idv". The second column contains a number or pointer that points to another portion of the record devoted to listing the transactions that ~~for which~~ the registered user has indicated are to require an idv. For example, the first row of the second column points to the portion of the record illustrated in Figure 9.

Please replace the paragraph beginning at page 17, line 6, with the following:

The fourth column contains space for storing information about the requesting party. This fourth column can contain communication origin information. Communication origin information is some code for identifying the requesting party. For example, the communication origin information could be the phone number, Internet address, fax number, or email address of the requesting party. In a preferred embodiment, this communication origin information is received by the server computer 100 at the time of receipt of the numerical identifier.

Please replace the paragraph beginning at page 18, line 17, with the following:

It is noted that the information in the table of Figure 10 is saved and archived for legal and audit purposes. The information stored in the table of Figure 10 can be valuable to track a party's ~~parties'~~ financial or other transactions. Furthermore, such information may be valuable to resolve a legal dispute about a particular transaction. For example, some events, like will signings, will be verified years after an event's date.

Please replace the paragraph beginning at page 19, line 7, with the following:

Returning to the operations of Figures 4a-c, once the idv list is linked to the registered user's record, the system is ready to be utilized in a transaction. The registered user armed with its list of idv's (obtained from the system in operation 409)

initiates a transaction by providing the requesting party with a numerical identifier and an unused idv from the registered user's list of idv's. The requesting party then submits the numerical identifier and the idv to the identity verification ~~verifier~~ system of this invention. As discussed earlier, the submission of the numerical identifier and the idv to the system can be done in many different ways including but not limited to by telephone, over the Internet, or via an electronic remote terminal similar to a credit card reader.

Please replace the five paragraphs beginning at page 21, line 1, with the following:

If an idv was received in receiving operation 410, then operation flows from operation 422 to determining operation 432. Determining operation 432 compares the received idv with the list of idv's in the registered user's record to determine whether the received idv is within the relevant range of the registered user's list of idv's. In other words, the determining operation 432 ~~only~~ searches idv's only within the relevant range. Implementation of the comparison may be accelerated by prior creation of a second sorted copy of the list of ~~if~~ idv's with pointers to the location of each idv in the original list.

If the idv received is not within the relevant ~~acceptable~~ range of the registered user's idv's, that is, if the idv received match none of the idv's in the relevant range of the registered user's list of idv's, then communication operation 434 sends a message to the requesting party indicating that an identity crime is potentially being committed.

If the idv received is within the relevant ~~acceptable~~ range of the registered user's idv's, that is, if the idv received matches one of the idv's in the relevant range of the registered user's list of idv's, then determining operation 436 compares the received idv with a list of idv's already used to determine whether the received idv has been used before.

As discussed above, idv character strings may be repeated as long as the repeat occurs outside a "relevant range". Therefore, the search in operation 436 of previously used idv's should ~~only~~ search only within the relevant range of the idv list.

If the received idv has been used before, then communications operation 438 sends a message to the requesting party indicating that the submitted idv has ~~already~~

been used before. There are two main possible reasons that an idv would have ~~already~~ been used before. First, the second attempt to use the idv could be an identity fraud attempt. Second, the type of transaction being performed might have two legitimate requesting parties. For example, in a payment by check type of transaction, the registered user may write out a check to a retailer and provide an idv to the retailer. The retailer submits the idv to the identity verification system and obtains verification of the registered user's identity (and receives a verification transaction identifier). The retailer then attempts to cash the check at a bank. The bank may submit the idv to the identity verification system. This submission would be a second use of the idv, but it would not be an attempted identity crime. The flow operations 438, 440, 441, 442 and 443 distinguish ~~distinguishe~~ between these two possible reasons for multiple idv use. Communications operation 438 requests submission of an earlier verification transaction identifier. Communications operation 438 may receive an earlier verification transaction identifier from the requesting party in response to the request.

Please replace the paragraph beginning at page 22, line 15, with the following:

Returning to determining operation 436, if the idv has not been used before[[,]] (within the relevant range), then operation flows to determining operation 444.

Please replace the two paragraphs beginning at page 22, line 22, with the following:

If a message is associated with the idv, then communicating operation 446 sends the message associated with the idv to the requesting party. At this point the requesting party can compare the message received from the system to the information received by the party providing the idv. If the message received from the system is not the same as ~~and~~ the information from the party providing the idv, then the requesting party can reasonably determine that fraud is being attempted and can therefore terminate the transaction.

Determining category operation 448 reviews information from the requesting party (received in the receiving operation 410) [[to]] and ascertains the category of the requesting party. This determining operation allows the system to

eventually release only the pre-authorized information in the registered user's record to the requesting party.

Please replace the paragraph beginning at page 23, line 15, with the following:

Archiving operation 452 stores the information from the transaction such as the numerical identifier and all associated record information. This storage of information can be done in the database or on ~~back of the~~ tapes or by other means. Archiving operation 452 results in the ability to audit and prove past transactions.